REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-15 and 17-26 are pending in the application. The Examiner additionally stated that claims 1-15 and 17-26 are rejected. By this communication, claim 1 is amended. Hence, claims 1-15 and 17-26 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §112

The Examiner rejected claim 1 under 35 U.S.C. 112, second paragraph for failing to point out and distinctly claim the subject matter which Applicant regards as his invention, noting that the claims recites the limitations "keygen logic" and "said plurality of input," yet providing no antecedent basis therefor.

In response, Applicant amends claim 1 by this communication to recite "keygen unit" and "a plurality of input," both of these limitations having sufficient antecedent basis in the claim. Accordingly, it is requested that the rejection of claim 1 be withdrawn.

Rejections Under 35 U.S.C. §102(e)

The Examiner rejected claims 22-25 under 35 U.S.C. 102(b) as being anticipated by Yup et al. (US2002/0191784), hereinafter, "Yup." Applicant respectfully traverses the Examiner's rejections.

As per claim 22, the Examiner wrote that Yup discloses a method for performing cryptographic operations in a device, the method comprising:

- Receiving a cryptographic instruction that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations (page 4, paragraph [0045]); and
- Employing the user-generated key schedule when executing the one of the cryptographic operations (page 3, paragraphs [0028-0035]).

The Examiner conceded that Yup does not explicitly disclose that the device is microprocessor, however, the Examiner noted that Kessler et al. discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2) and, therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup et al to be a processor, and that one would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Applicant respectfully submits that the rejection is improper under 35 U.S.C. 102(e) for the Examiner has cited more than a single reference in her arguments and, thus, (e) the invention is "not described in (1) an application for patent, published under section 122 (b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant." Accordingly, it is requested that the rejection of claim 22 be withdrawn.

Claims 23-25 depend from clam 22 and add further limitations over that subject matter which is argued above as being allowable. Consequently, it is requested that the rejections of claims 23-25 be withdrawn as well.

In deference to the Examiner, Applicant assumes that it was the Examiner's intention to reject claims 22-25 under 35 U.S.C. 103(a) rather than under 35 U.S.C. 102(e). Accordingly, arguments supporting allowance of these claims will be submitted hereinbelow.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 8-15, and 17-20 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Kessler et al. (US 6789147), hereinafter, "Kessler." Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup discloses an apparatus for performing cryptographic operations, comprising:

- An instruction register having a cryptographic instruction, received by microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations (page 4, paragraph [0045]);
- A keygen unit, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to load said user-generated key schedule (page 3, paragraph [0028]).
- An execution unit, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations, said execution unit comprising:
    - A cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (page 1, paragraph [0004]).

The Examiner conceded that Yup does not explicitly disclose that the device is microprocessor, but that Kessler discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). The Examiner therefore concluded that it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup at al to be a processor, for one would have been

motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Applicant respectfully disagrees with the Examiner's characterization and understanding of the prior art, the invention as recited in claim 1, and furthermore with the Examiner's understanding, as argued in the instant office action, of the area of the art that includes processors, microprocessors, CPUs, and coprocessors. Thus, the following points are submitted in traversal of the rejection.

First, one skilled in the art will concur that a microprocessor includes an understood set of functions and logic elements. Generally speaking, a microprocessor is understood by those in the art to microprocessor be a programmable digital electronic component that incorporates the functions of a central processing unit (CPU) on a single integrated circuit (IC). The aforementioned aspects of the microprocessor according to the present invention are very adequately disclosed within the instant application to include the ability to fetch and execute instructions that have been provided in an application program, to perform address translation, to load and store variables from/to memory, etc. As such, a microprocessor differs from a coprocessor, which is conventionally understood to supplement the functions of the CPU. Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption, as has been discussed in the instant application. Coprocessors require the host main processor to fetch the coprocessor instructions and handle all other operations aside from the coprocessor functions. Accordingly, and as Applicant has discussed in the instant application, a microprocessor is not a coprocessor, nor is a coprocessor a microprocessor. Applicant has discussed the existence and disadvantages of present day cryptographic coprocessors, and has provided the present invention to overcome the disadvantages of such.

The apparatus of Yup is not even a coprocessor. It is a circuit. Yup does not even mention or hint that his circuit may be construed as a coprocessor. Certainly, Yup does not disclose, suggest, allude to, or even hint that his circuit be construed or combined with other circuits to yield a coprocessor, much less a microprocessor.

Applicant has specifically recited that the instruction register having a cryptographic instruction disposed therein is *received by a microprocessor.* Such terminology is well understood and appreciated by one of ordinary skill in the art, and it is respectfully submitted that to equate a circuit as disclosed by Yup, or even a coprocessor, with a microprocessor does not reflect an understanding of the terminology of the art. In summary, among other novel aspects and features, the technique according to the present invention provides a cryptographic instruction that a programmer can employ to directly program cryptographic operations into an application program, where such operations are performed by a microprocessor that provides a cryptography unit within its execution logic. This microprocessor is not a coprocessor, nor is it a simple circuit.

With the above summary in view, Applicant respectfully submits that claim 1 recites an instruction register having a cryptographic instruction disposed therein. Yup does not recite an instruction register, nor does he disclose a cryptographic instruction. In contrast, Yup teaches a circuit being coupled to a system having a plurality of channels. The circuit 100 includes a plurality of input registers 102, one each coupled to the plurality of system channels. The input registers 102 are preferably simple first-in/first-out (FIFO) registers. The input registers 102 each receive a data string of a first predetermined bit length from its corresponding system channel. In the preferred embodiment, the predetermined bit length is 64 bits. The circuit 100 also includes a plurality of control signal input lines 103, one for each channel, coupled to receive control signals from systems and circuits external to the circuit 100. (Paragraphs 24-25)

Clearly, the circuit of Yup could be employed to perform AES encryption and decryption, but his circuit must be totally controlled via the input registers 102 and the control signal input lines 103. This is the way to perform these operations on the circuit of Yup.

In addition, claim 1 recites that a keygen unit and an execution unit are coupled to the instruction register in the microprocessor. The execution unit includes a cryptography unit that executes execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks.

Yup does not teach these elements within a microprocessor because Yup does not teach or suggest a microprocessor at all, but rather a circuit that must be driven by control signal lines and provided with data over system channels.

The Examiner's concession that Yup does not explicitly disclose that the device is microprocessor is accepted, but Applicant wishes to argue further that Yup, by his lack of recitation of any of the functions normally attributed to a CPU, also explicitly teaches that his devices is *not* a microprocessor. It is only a circuit. Applicant accepts the Examiner's assertion that that Kessler discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). However, Applicant wishes to direct the Examiner's attention to FIGURE 2 of Kessler, where he explicitly depicts that his "cryptographic processor" includes both a host processor 202 and a co-processor 212. These two units communicate with one another over a system bus 210. And Kessler himself uses the term "CPU" interchangeably with "host processor" (col. 2, line 33) where he discusses the existence and need for better interfaces with a security coprocessor. Thus, Kessler teaches a technique to allow for more efficient interface to a security coprocessor.

Thus, it does not follow that one skilled in the art would combine the teachings of Kessler with Yup to yield a *microprocessor*. Actually, the Examiner's exact words were that one skilled would construe the device described in Yup at al to be a processor, for one would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design. In the sense that Kessler teaches a "processor" (Fig. 2) to include both a host processor *and* a security *coprocessor* that are coupled together by a system bus, Applicant respectfully asserts one skilled in the art might be motivated by these two disclosures to employ the *circuit* of Yup within the *coprocessor* of Kessler to perform AES encryption and decryption, but these two references, alone or in combination, utterly fail to suggest a microprocessor as is recited in claim 1.

Accordingly, it is respectfully requested that the rejection of claim 1 be withdrawn.

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a

combination of Yup and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

As per claim 17, the Examiner opined that Yup discloses an apparatus for performing cryptographic operations, comprising:

- A cryptography unit within a microprocessor, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes a key size to be employed when executing said one of the cryptographic operations (AES block cipher can use varying key lengths) [page 4, paragraph 0045];
- A keygen unit, operatively coupled to said cryptography unit, configured to direct said microprocessor to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations (page 3, paragraph [0028].

The Examiner also noted that Yup does not explicitly discloses that the device is microprocessor, but that Kessler discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2) and, therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup et al to be a processor, noting that one would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Applicant respectfully traverses the rejection and directs the Examiner's attention to arguments submitted above in traversal of the rejection of claim 1. In summary, as recited in claim 1, claim 17 specifically recites a *microprocessor*. This is not a generic term, such as "processor," but is an art-specific construct which can stand alone, but which is adequately supported within the instant disclosure to connote a programmable CPU on a single integrated circuit. Consequently, while Yup discloses a "circuit," and Kessler discloses a "processor" comprising both a host processor (CPU) and coprocessor,

neither of these references remotely suggest a microprocessor that consists of the elements recited in claim 17.

Accordingly, it is respectfully suggested that the rejection of claim 17 be withdrawn as well.

With respect to claims 18-20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a combination of Yup and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

Applicant also respectfully submits that claim 22 recites a method for performing cryptographic operations in a *microprocessor* and within a cryptographic unit *in the microprocessor*. Neither of these two limitations can be met or suggested by the teachings of Yup or Kessler. Accordingly, it is submitted that claim 22 is allowable as well.

Claims 23-25 depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a combination of Yup and Kessler. Accordingly, Applicant respectfully submits that claims 23-25 are allowable as well.

The Examiner also rejected claims 7 and 21 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Kessler, and further in view of Miller (US 6081884), hereinafter, "Miller." Applicant respectfully traverses the rejections and notes that claims 7 and 21 depend from claims 1 and 17, respectively, and add further limitations over that subject matter which has been argued above as being allowable over the cited references. Accordingly, it is requested that the rejections of claims 7 and 21 be withdrawn.

The Examiner furthermore rejected claim 26 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Kessler, and further in view of Miller (US 6081884), hereinafter, "Miller." Applicant respectfully traverses the rejections and notes that claim 26 depends from claim 22, and adds further limitations over that subject matter which has been argued above as being allowable over the cited references. Accordingly, it is requested that the rejection of claim 26 be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-15 and 17-26 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

01/07/2008

Date: _____